(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06315027 A**

(43) Date of publication of application: **08.11.94**

(51) Int. Cl **H04L 9/06**
H04L 9/14
G09C 1/00

(21) Application number: **06049081**

(22) Date of filing: **18.03.94**

(30) Priority: **23.04.93 US 93 52304**

(71) Applicant: **INTERNATL BUSINESS MACH CORP <IBM>**

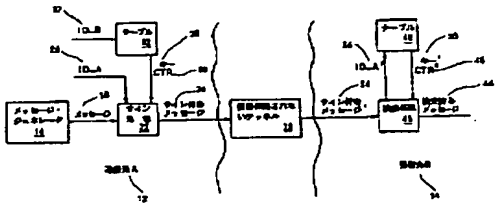
(72) Inventor: **BELLARE MIHIR**
GUERIN ROCH ANDRE
ROGAWAY PHILLIP WALDER

(54) **METHOD AND DEVICE FOR DATA AUTHENTICATION IN DATA COMMUNICATION ENVIRONMENT**

(57) Abstract:

PURPOSE: To obtain an improved data processing system by generating a tag by combining plural cryptographic words and deciding an authentication tag used with data transfer in which a communication channel is used.

CONSTITUTION: A message is signed by a transmitting origin 12 by a sign processing 22. A message 18, a transmitting origin identifier 26, a shared key 28 and a counter 30 are received by the processing 22. A message 24 with a signature is transmitted with a channel 20. A message 34 is received and an identifier 36 of a signer is extracted by inspecting the message 34 by a receiving destination 14. A value of the receiving destination itself of a key 38 of the receiving destination itself shared by a person who is provided with the identifier equal to the identifier 36 and a value of the receiving destination itself of a CTR 45 is looked up by using the identifier 36 by using a table 42 indexed by the identifier 36 by the receiving destination. After that, the message 34, the identifier 36, the key 38 and the CRT 45 are taken, inspection completion message 44 is recovered or the message 34 is judged to be forged by an inspection processing 43 and when the message 34 is judged to be forged, the message is discarded.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平6－315027
(43)公開日　平成６年(1994)11月８日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ 9/06				
9/14				
Ｇ０９Ｃ 1/00		8837－5Ｌ		
		8949－5Ｋ	Ｈ０４Ｌ 9/ 02	Ｚ

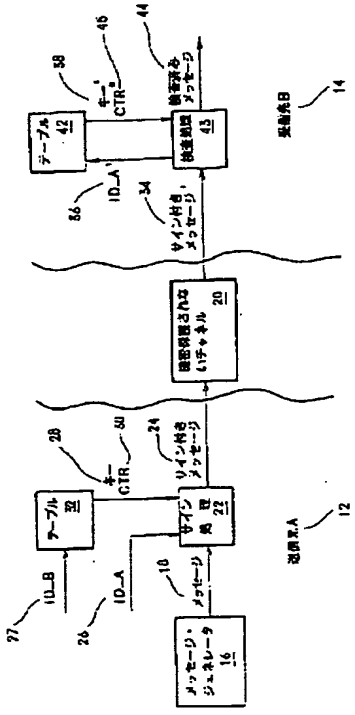
審査請求　有　請求項の数44　ＯＬ　（全 19 頁）

(21)出願番号　特願平6－49081
(22)出願日　平成６年(1994)３月18日
(31)優先権主張番号　０５２３０４
(32)優先日　1993年４月23日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(72)発明者　ミヒル・ベラーレ
アメリカ合衆国10025　ニューヨーク州ニューヨーク　セントラル・パーク・ウェスト372　ナンバー16イー
(74)代理人　弁理士　合田　潔　（外２名）
最終頁に続く

(54)【発明の名称】　データ通信環境におけるデータ認証のための方法および装置

(57)【要約】
【目的】　データ通信環境内で、単純、高速かつ安全にデータ認証を提供するためのシステムおよび方法を提供すること。
【構成】　転送するデータ・メッセージを、データ・ブロックに分割する。各データ・ブロックをブロック・インデックスと組み合わせて、ワードを作成する。各ワードに擬似乱数関数を適用して、複数の暗号データ列を作成する。送信元の識別子とカウンタ値を含む識別子用ヘッダも、擬似乱数関数を使用して暗号化する。この暗号化されたデータ列とヘッダを論理的に組み合わせて、タグを作成する。特定のワードの暗号化は他のワードと独立に行われるので、各ブロックを他のブロックとは独立に暗号化することができる。したがって、この方法およびシステムは、並列にまたはパイプライン方式で実行でき構成できる。受信側の構成要素またはシステムは、メッセージ信頼性を判定するために送信されたタグと比較することのできる、第２のタグを生成する。



1

【特許請求の範囲】

【請求項１】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【請求項２】前記擬似乱数関数が、データ暗号化標準（ＤＥＳ）アルゴリズムであることを特徴とする、請求項１の方法。

【請求項３】前記ブロックが、固定長であることを特徴とする、請求項１の方法。

【請求項４】前記組み合わせステップが、排他的論理和演算を含むことを特徴とする、請求項１の方法。

【請求項５】前記タグが、切捨てその他の方法によって所与の長さに短縮されることを特徴とする、請求項１の方法。

【請求項６】前記擬似乱数関数が、多段式であることを特徴とする、請求項１の方法。

【請求項７】前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、請求項６の方法。

【請求項８】前記複数のワードが、前記複数の多段式擬似乱数関数に同時に提示されることを特徴とする、請求項１の方法。

【請求項９】さらに、少なくとも前記タグを前記識別子と組み合わせて、メッセージ認証コード（ＭＡＣ）を作成するステップを含む、請求項１の方法。

【請求項１０】さらに、少なくともデータとメッセージ認証コードとを組み合わせて、データ・パケットを作成するステップを含む、請求項９の方法。

【請求項１１】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

（ｉ）前記ワードのそれぞれと（ii）前記データのヘッダとに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、メッセージ認証コード（ＭＡＣ）を作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【請求項１２】前記擬似乱数関数が、データ暗号化標準（ＤＥＳ）アルゴリズムであることを特徴とする、請求項１１の方法。

2

【請求項１３】前記ブロックが、固定長であることを特徴とする、請求項１１の方法。

【請求項１４】前記組み合わせステップが、排他的論理和演算を含むことを特徴とする、請求項１１の方法。

【請求項１５】前記ヘッダが、識別子とカウンタとを含むことを特徴とする、請求項１１の方法。

【請求項１６】前記タグが、切捨てによって所与の長さに短縮されることを特徴とする、請求項１１の方法。

【請求項１７】前記擬似乱数関数が、多段式であることを特徴とする、請求項１１の方法。

【請求項１８】前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、請求項１７の方法。

【請求項１９】前記複数のワードが、前記複数の多段式擬似乱数関数に同時に提示されることを特徴とする、請求項１１の方法。

【請求項２０】さらに、少なくとも前記タグを前記識別子と組み合わせて、メッセージ認証コード（ＭＡＣ）を作成するステップを含む、請求項１１の方法。

【請求項２１】さらに、少なくともデータとメッセージ認証コードとを組み合わせて、データ・パケットを作成するステップを含む、請求項２０の方法。

【請求項２２】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、タグを作成するステップと、

少なくとも前記データと前記タグとを組み合わせて、データ・パケットを作成するステップと、

非機密保護通信チャネルを介して前記データ・パケットを送信するステップと、

データ・パケットを受信するステップと、

データ・パケットを分解して、タグとデータを抽出するステップと、

少なくとも抽出されたデータと局所キーとから第２タグを生成するステップと、

抽出されたタグと第２タグを比較して、データ・パケットのデータ信頼性を判定するステップとを含む、非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【請求項２３】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれにブロック識別子を連結して、ワードを作成するステップと、

前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

3

前記複数の暗号ワードを組み合わせて、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【請求項２４】前記ブロック識別子が、ブロック・インデックスに基づくことを特徴とする、請求項２３の方法。

【請求項２５】前記擬似乱数関数が、多段式であることを特徴とする、請求項２３の方法。

【請求項２６】前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、請求項２５の方法。

【請求項２７】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

（ｉ）前記ワードのそれぞれと（ii）前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、タグを作成するステップと、

少なくともデータとタグとを組み合わせて、データ・パケットを作成するステップと、

非機密保護通信チャネルを介してデータ・パケットを送信するステップと、

データ・パケットを受信するステップと、

受信したデータ・パケットを分解して、受信データと受信タグを抽出するステップと、

少なくとも受信データと局所キーとから局所タグを生成するステップと、

受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【請求項２８】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

（ｉ）前記ワードのそれぞれと（ii）前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、タグを作成するステップと、

少なくともデータ、タグ、送信元識別子および時間変動パラメータを組み合わせて、データ・パケットを作成するステップと、

非機密保護通信チャネルを介してデータ・パケットを送信するステップと、

データ・パケットを受信するステップと、

4

受信データ・パケットを分解して、受信データ、受信タグ、受信送信元識別子および受信時間変動パラメータを抽出するステップと、

少なくとも受信データ、受信送信元識別子、受信時間変動パラメータおよび局所キーから局所タグを生成するステップと、

受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、前記非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【請求項２９】前記比較ステップが、さらに、前記受信時間変動パラメータを局所時間変動パラメータと比較して、前記データ信頼性をさらに判定するステップを含むことを特徴とする、請求項２８の方法。

【請求項３０】前記受信時間変動パラメータが、受信カウンタを含むことを特徴とする、請求項２９の方法。

【請求項３１】前記受信時間変動パラメータが、タイム・スタンプを含むことを特徴とする、請求項２９の方法。

【請求項３２】前記受信時間変動パラメータが、シーケンス番号を含むことを特徴とする、請求項２９の方法。

【請求項３３】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれにブロック識別子を連結して、ワードを作成するステップと、

（ｉ）前記ワードのそれぞれと（ii）前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【請求項３４】受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出するステップと、

少なくとも受信データ、受信時間変動パラメータおよび局所キーから局所タグを生成するステップと、

受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、受信データ・パケットの信頼性を判定するための方法。

【請求項３５】前記受信時間変動パラメータが、受信カウンタを含むことを特徴とする、請求項３４の方法。

【請求項３６】前記受信時間変動パラメータが、タイム・スタンプを含むことを特徴とする、請求項３４の方法。

【請求項３７】前記受信時間変動パラメータが、シーケンス番号を含むことを特徴とする、請求項３４の方法。

【請求項３８】前記受信データ・パケットが、さらに送信元識別子を含むことを特徴とする、請求項３４の方法。

【請求項３９】さらに、前記送信元識別子を使用して、

5

局所テーブルから前記局所キーを取得するステップを含む、請求項３８の方法。

【請求項４０】データを複数のブロックに区分する手段と、

前記ブロックのそれぞれを符号化して、前記ブロックのそれぞれの値と前記ブロックのそれぞれの識別子との両方を表すワードを作成する手段と、

前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、

前記複数の暗号ワードを組み合わせて、タグを作成する手段とを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するためのシステム。

【請求項４１】データを複数のブロックに区分する手段と、

前記ブロックのそれぞれにブロック識別子を組み合わせて、ワードを作成する手段と、

（ｉ）前記ワードのそれぞれと（ii）前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、

前記複数の暗号ワードを組み合わせて、タグを作成する手段とを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するためのシステム。

【請求項４２】受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出する手段と、

少なくとも受信データ、受信時間変動パラメータおよび局所キーから局所タグを生成する手段と、

受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定する手段とを含む、受信データ・パケットの信頼性を判定するためのシステム。

【請求項４３】前記受信データ・パケットが、さらに送信元識別子を含むことを特徴とする、請求項４２のシステム。

【請求項４４】さらに、前記送信元識別子を使用して、局所テーブルから前記局所キーにアクセスする手段を含む、請求項４３のシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、データ通信手順に関し、具体的には、機密保護されない通信媒体を使用する際に認証済みデータを提供するための手順に関する。

【０００２】

【従来の技術】通信システムでは、一般に、２人の当事者が、機密保護されないチャネルを介して、一方の当事者が受け取ったメッセージが実際に他方の当事者が作成したものであることを各当事者が確信できる形で通信できることを望む。機密保護されないチャネルとは、第３者が、通信リンクを通過するメッセージ・トラフィックを監視または調査でき、かつ自分自身のメッセージを挿入できるチャネルである。通信中の２人の当事者は、短

6

いランダムな秘密キーを所有している、または取得できると仮定することができる。機密保護されないチャネルを介してこのような通信を達成するために、当技術分野ではさまざまな技法が知られている。たとえば、その技法は、Ｒ．ジュメマン（Juememan）、Ｓ．マチアス（Matyas）、Ｃ．マイヤー（Meyer）の論文"Message Authentication", IEEE Communications、１９８５年９月等に記載されている。既知の技法の１つでは、各当事者が、送ろうとする各メッセージに、メッセージと秘密キーとおそらくは他の引数との関数として計算される、短いメッセージ認証コード（ＭＡＣ：Message Authentification Code）を付加する。

【０００３】このタイプのシステムは、たとえば、ＡＮＳＩのＸ９．９標準（ＡＮＳＩ　Ｘ９．９、１９８２）によって示されるように、当技術分野で既知である。しかし、このシステムには、ＭＡＣを計算できる速度が、その基礎となる暗号動作を実行できる速度によって制限されるという欠点がある。ＡＮＳＩ　Ｘ９．９の機構を示す図１０に示されるように、この制限は、この機構の逐次式という性質に起因するものである。この機構は、メッセージをブロックに分割し、ブロックを暗号化し、暗号化されたブロックとメッセージの次ブロックの排他的論理和をとり、その結果を暗号化し、すべてのブロックの処理が終わるまでこれを繰り返すことからなっている。したがって、あるブロックを利用するためには、その前のすべてのブロックが指定に従って暗号化され排他的論理和をとられるまで、待機しなければならない。この逐次式処理は、ブロックの到着速度が単一ブロックの処理に必要な時間の逆数より速い、超高速のネットワークで問題になる。このようなネットワークでは、余分のハードウェアを設けても、ＭＡＣの計算を高速化するのには役立たない。というのは、ボトルネックの原因が、暗号プリミティブの計算に要する時間であって、その計算を行うための資源の不足ではないからである。このようなネットワークでは、暗号プリミティブを計算できる速度に合わせて、送信時間を低速化する必要が生じるはずである。したがって、高速ネットワークでの全体的システム・スループットは、このタイプの逐次式メッセージ・タグ計算によって大きな影響を受け、情報転送の効率が低下する可能性がある。

【０００４】

【発明が解決しようとする課題】本発明の目的は、改良されたデータ処理システムを提供することである。

【０００５】本発明のもう１つの目的は、データ処理システム用の改善されたデータ転送手順を提供することである。

【０００６】本発明のもう１つの目的は、非機密保護通信環境でのデータ用の改良された認証システムを提供することである。

【０００７】本発明のもう１つの目的は、データ処理シ

ステムで転送されるメッセージの認証に使用されるメッセージ認証コードを決定するための、改善された方法を提供することである。

【０００８】

【課題を解決するための手段】本発明は、簡単かつ高速でおそらくは安全にメッセージ認証コード（ＭＡＣ）を計算する方法を提供する。送ろうとするデータを、データ・ブロックに分割し、このデータ・ブロックに連続したインデックス１、２、３、…、ｎを付ける。各ブロックｉについて、ブロックｉの内容とインデックスｉ（識別子）を符号化することによってワードｘｉを作成する。各ワードｘｉにそれぞれ擬似乱数関数を適用して、暗号ワードｙｉを作成する。さらに、送信元の識別子とカウンタを符号化することによって、識別子用シーケンス番号ｘ０（ヘッダ）を作成する。識別子用ヘッダｘ０に擬似乱数関数を適用して、暗号ヘッダｙ０を生成する。これらの暗号ワードと暗号ヘッダを論理的に組み合わせて、タグｔを作成する。タグｔは、送信元の識別子（ＩＤ＿Ａ）およびカウンタの値（ＣＴＲ）と共に、メッセージ認証コードを形成する。好ましい実施例では、擬似乱数関数がデータ暗号化標準（ＤＥＳ）のアルゴリズムであり、ブロック・サイズなどはそれに従って選択される。

【０００９】擬似乱数関数はそれぞれのワードに他のワードと独立に適用されるので、擬似乱数関数の計算は、ワードｘｉごとに独立に（たとえば並行にまたはパイプライン式に）実行できる。したがって、この方法およびシステムは、並行にまたはパイプライン式に実行でき構成できる。タグのサイズは、メッセージ長と独立である。受信側の構成要素またはシステムは、メッセージの信頼性を判定する際に送信されたタグと比較できる、第２のタグを生成する。

【００１０】

【実施例】図１を参照すると、送信元１２が、メッセージまたはデータをある受信先１４に安全に送信しようと試みている。この送信元および受信先は、コンピュータ、通信カード、交換機または他の計算実体とすることができる。メッセージ・ジェネレータ１６が、送信元１２用のメッセージを作成している。このメッセージの内容を、機密保護されないチャネル２０を介して受信先１４に送信しなければならない。メッセージ・ジェネレータ１６は、たとえば、通信スタックの下位層実体、上位層アプリケーション実体、音声データまたはビデオ・データの供給源もしくは他のデータ供給源とすることができる。機密保護されないチャネル２０は、たとえば、物理的に露出されたワイヤ、光ファイバ・ケーブル、無線ＬＡＮ、衛星チャネルなどとすることができる。

【００１１】受信先１４は、送信元１２によって送られたと主張されるメッセージが実際にその送信元によって送られたと確認したいと思う。この目的のため、送信元

は、サイン処理２２でメッセージにサインする（すなわち、メッセージを認証する）。こうしてメッセージにサインすることで、サイン付きメッセージ２４が生じる。サイン処理２２は、メッセージ（message）１８、送信元の識別子（ＩＤ＿Ａ）２６、送信元と受信先で共用されるキー（key）２８、およびカウンタ（ＣＴＲ）３０を受け取る。キーとＣＴＲは、送信元および受信先の識別子に（テーブル３２を介し標準技法を使用して）関連付けられ、この両方が以下でさらに説明するタグ計算に使用される。好ましい実施例では、関連するキー２８およびＣＴＲ３０が、テーブル３２に記憶され、受信先の識別子であるＩＤ＿Ｂ　２７によってインデックスされるものとして示されている。この場合、これらの値を、サイン処理２２が当技術分野で既知の普通のインデックス技法を使用して獲得することができる。

【００１２】サイン付きメッセージ２４は、機密保護されないチャネル２０を介して送信される。このチャネルのもう一方の端で、あるサイン付きメッセージ'（signed message'）３４が受信先１４によって受信される。このサイン付きメッセージ'３４は、サイン付きメッセージ２４と同一であってもそうでなくてもよい。たとえば、この伝送に使用される機密保護されないチャネル（channel）２０は機密保護されていないので、送信元１２が実際にはサイン付きメッセージ２４を送信していないのに、サイン付きメッセージ'３４が受信される可能性がある。あるいは、侵入者が、サイン付きメッセージのビットをいくつか変更している可能性もある。

【００１３】受信先１４は、サイン付きメッセージ'３４を受信し、そのサイン付きメッセージ'を検査することによって、そこで主張された署名者の識別子ＩＤ＿Ａ'３６を抽出する。受信先は、ＩＤ＿Ａ'によってインデックスされるテーブル４２を使用することにより、ＩＤ＿Ａ'３６を使用して、ＩＤ＿Ａ'に等しい識別子を有する者と共用する受信先自体のキー'３８と、ＣＴＲ'４５の受信先自体の値を表引きする。その後、検査処理４３が、サイン付きメッセージ'３４、ＩＤ＿Ａ'３６、キー'３８およびＣＴＲ'４５を取り、検査済みメッセージ４４を回復するか、あるいはサイン付きメッセージ'３４が偽造であると判断する。偽造が検出された場合、そのメッセージは廃棄され、他の適当な処置をとることができる。

【００１４】図２に、図１のサイン処理２２を詳細に示す。このサイン処理２２は、メッセージ１８を受け取り、ブロック４６で、このメッセージを、送信元の識別子であるＩＤ＿Ａ　２６、カウンタの現在値であるＣＴＲ　３０およびタグ４８と連結し、あるいはその他の方法で組み合わせ、符号化する。ＣＴＲ値は、ブロック５４で、テーブル３２（図１）から読み取られる。タグ計算５６については後で図４を参照して説明するが、これは、ブロック６０でのテーブル３２（図１）からのキー

9

２８の読取りを含む。結果として得られる連結された文字列、Ｍｅｓｓａｇｅ．ＩＤ＿Ａ．ＣＴＲ．Ｔａｇ５８が、図１のサイン付きメッセージ２４である。このサイン付きメッセージに組み合わされたＩＤ＿Ａ．ＣＴＲ．Ｔａｇ部分（すなわち、メッセージ自体を除くすべて）が、図８の符号８６に示されるメッセージ認証コード（ＭＡＣ）である。

【００１５】各メッセージのサイン処理のたびに、ブロック６２で、カウンタＣＴＲの現在値が増分され、あるいは新しい値に変更される。この値は、ブロック６４でテーブル３２（図１）にセーブされ、ＩＤ＿Ａから発する次のメッセージの認証またはサインに使用される。

【００１６】ここで図３を参照すると、サイン付きメッセージ'３４が、受信先１４に入ってくる。ブロック６６でこのメッセージを分解して、それを構成するメッセージ'３５、ＩＤ＿Ａ'３６、ＣＴＲ'４０およびタグ'４１を決定する。ブロック４７で、ＩＤ＿Ａ'３６を使用してテーブル４２（図１）をインデクシングして、局所キーであるキー'３８を得る。ブロック６８で、メッセージ'３５、ＩＤ＿Ａ'３６、ＣＴＲ'４０およびキー'３８を使用し、送信元１２が図２のタグ４８を計算するのに使用したタグ計算５６と同じアルゴリズムを使用して、受信先１４が、この受信したサイン付きメッセージ'３４に適したタグ"（ＴＡＧ"）７０を計算する。ブロック７２で、ブロック６８で計算したタグ"７０が受信したタグ'４１と異なると判定される場合、この受信された送信は真正ではないとみなされ、ブロック７４で廃棄される。タグが一致する場合、ブロック７３でテーブル４２（図１）からＣＴＲ"４５を読み取った後に、ブロック７６で、受信したカウンタＣＴＲ'４０を受信先自体のカウンタであるＣＴＲ"４５と比較する。前者のほうが大きい場合、ブロック７８でこのメッセージを受け入れ、ブロック８０で受信先のカウンタＣＴＲ"４５をＣＴＲ'の値で置き換え、ブロック８２でテーブル４２（図１）に書き込む。そうでない場合、受信した送信は真正でないとみなされ、ブロック７４で廃棄される。

【００１７】時間変動パラメータＣＴＲ"４５の重要性は、所与のＣＴＲ'値に対してあるメッセージを受け入れた後に、同じＣＴＲ値で追加のメッセージを受け入れないようにすることである。好ましい実施例では、メッセージごとに増分されるカウンタを使用し、ＣＴＲの最近の値だけをセーブするだけで、カウンタ値が複製されないようにする。しかし、送信されたメッセージが送信時の順序と異なる順序で受信される場合には、これが問題をもたらす。この問題は、真正であるとみなされたメッセージ上で受信された最大のＣＴＲ'値からなるｋ要素の集合Ｓを受信先がセーブすることによって解決される。さらに、受信先は、（前に説明したように）値ＣＴＲ"をセーブする。あるメッセージは、そのＣＴＲ'値が

10

集合Ｓに含まれるか、あるいはＣＴＲ"以下のＣＴＲ'値を有する場合に、再生（すなわち真正でない）と判定される。真正のメッセージを受信した時、そのＣＴＲ'値を集合Ｓに追加し、ＣＴＲ"をその集合の最小要素で置き換え、その後、Ｓの最小要素をＳから取り除く。これによって、複製ＣＴＲ'値が有効として受け入れられないことが保証される。

【００１８】別法として、タイム・スタンプなど他のタイプの時間変動パラメータをカウンタの代わりに使用することもできる。送信元は、前述のＣＴＲの代わりに、その現在時刻ＴＩＭＥを使用する。受信先は、受信先の現在時刻ＴＩＭＥ"からあるデルタ量の範囲内にあり、既に使用された時刻値の集合Ｓのどの時刻値ＴＩＭＥ'とも異なる、ＴＩＭＥ'値を受け入れる。時刻値ＴＩＭＥ'は、このＴＩＭＥ'値を使用してメッセージが受け入れられる時、この集合Ｓに入れられる。ＴＩＭＥ'値は、受信先の現在時刻ＴＩＭＥ"との差がデルタ量を越える時、集合Ｓから取り除かれる。同様の技法を使用して、ブロック・シーケンス番号を時間変動パラメータとして使用することもできる。

【００１９】図４は、当技術分野で既知のデータ暗号化標準（ＤＥＳ）のアルゴリズムに基づく、図２のタグ計算５６と図３のタグ計算６８の１実施例を示す図である。この暗号化標準は、たとえば、Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, D.C., １９７７年１月に記載されている。図４に示した方法に関する前提条件は次のとおりである。第１に、キー２８（図１）を使用してメッセージを送る実体が１つだけ存在し、したがって、その識別子ＩＤ＿Ａ　２６（図１）は、単にビット０として扱われる。第２に、キーの下で送られるメッセージは、2^{62}個未満である（その後、キーは、手動によりまたは自動的に新しいキーに更新される）。第３に、各メッセージは、長さが2^{31}個の３２ビット・ワード未満である。キーの下で送ることのできるメッセージの数は、カウンタに許容されるビットの数（好ましい実施例では６２ビット）によって決まる。１メッセージ内の３２ビット・ワードの数は、2^{31}を上限とする。というのは、この方式ではビット０がブロック・インデックスの前に付加され、３１ビットだけがブロック・インデックス／識別子の記述用に残されるからである。

【００２０】さらに具体的に図４を参照すると、メッセージ／データ８４は、Ｋ＝３２ビットの倍数になるように、何らかの標準的な方法で埋め込まれる。この埋込みはデータ処理分野で公知であるので、図４には示さない。メッセージ／データ８４は、ある個数ＮのＫビット・ブロックからなるとみなされる。図４には、Ｎ＝３ブロック（１２０、１２２および１２４）でＫ＝３２ビットの場合のメッセージ／データ８４の例が示されてい

る。

【００２１】各ブロック識別子の３２ビット符号化を、符号８８に示す。好ましい実施例では、この符号化の最初のビットが０にセットされ、残りのビットは、当該の各ブロックの整数値ｉ（ブロック・インデックス）の標準２進符号化である。符号９０にＭｉと示される、このメッセージのｉ番目の３２ビット・ブロックを、ブロック９２でブロック識別子８８の末尾に連結する。その結果得られるＮ個の６４ビット・ブロック８９を、ブロック９３で、暗号化標準（ＤＥＳ）のアルゴリズムを使用して、それぞれ暗号化する。それぞれの場合に使用されるキー９６は、このタグ計算を行うのが送信元と受信先のどちらであるかに応じて、キー２８またはキー'３８になる。その結果得られるＮ個の暗号テキスト９９のすべてが、ブロック９８で、もう１つの暗号テキスト１０２と共に、ビットごとに排他的論理和をとられる。この追加の暗号テキスト１０２は、下記のようにして生成される。

【００２２】追加の暗号テキスト１０２は、カウンタ１０４をワードの下位６２ビットに２進符号化することによって形成される。このカウンタ（このタグ計算を実行するのが送信元と受信先のどちらであるかに応じて、図１のＣＴＲ３０またはＣＴＲ'４０）の前に、ビット"１"（最上位ビット位置）と送信元の識別子（この動作が送信元と受信先のどちらで発生するのかに応じてＩＤ＿ＡまたはＩＤ＿Ａ'になり、好ましい実施例では１ビット長と仮定される）を連結したものが付加される。最上位ビット群の先頭ビットは、送信元のＩＤ／ＣＴＲを符号化するワードの空間を、メッセージ・ブロックを符号化する空間から分離するためのものである。最上位から２番目のビットは、送信元の識別子を示すためのものである。空間の分離によって、復号部分が、カウンタ・ブロックとメッセージ・ブロックを識別し、これらを区別できるようになる。というのは、前者は必ずビット１で始まり、後者は必ずビット０で始まるので、これらの組は決して共通要素をもたないからである。その結果得られる６４ビット・ワード９１は、ブロック１１０で暗号化基準のアルゴリズムを使用して暗号化される。この暗号テキスト１０２と他のＮ個の暗号テキスト９９の排他的論理和をとった後に、その結果得られる６４ビット文字列を、ブロック１１２でより少ないビット数に切り捨てる。図では３２ビットに切り捨てられている。もちろん、この切捨ては、代替実施例ではブロック９８の排他的論理和の前に行うことができる。その結果得られるタグ１１４は、このタグ計算を実行するのが送信元と受信先のどちらであるかに応じて、図２のタグ４８または図３のタグ'７０になる。

【００２３】上で説明した方法の多くを変更して、簡単に下記のものを含む代替実施例を得ることができる。

・別個の番号を有するブロックが異なる符号化を引き起こす限り、ブロック識別子８８と符号９０で示される３２ビット・ブロックからなるメッセージ・ブロックをどのように符号化してもよい。

・Ｒ．リヴェスト（Rivest）等の論文"The MD5 Message-Digest Algorithm", Network Working Group RFC 1321, １９９２年４月に記載のハッシュ関数である、ＭＤ５に基づく擬似乱数関数など、他の機構をＤＥＳの代わりに使用することができる。擬似乱数関数は、当技術分野で一般に知られており、たとえば、Ｏ．ゴールドライヒ（Goldreich），Ｓ．ゴールドヴァッサー（Goldwasser），Ｓ．ミカリ（Micali）の論文"How to Construct Random Functions", Journal of the Association for Computing Machinery, Vol. 33, No. 4, １９８６年１０月、782-807ページに記載されている。

・ＩＤ１０６とカウンタ（ＣＴＲ）１０４の符号化は、そのＩＤ／ＣＴＲ符号化が、番号付きメッセージ・ブロックの符号化空間と異なる空間に含まれる限り、すなわちすべてのｉ、ｍに関して＜ＩＤ＿Ａ、ＣＴＲ＞が＜ｉ、ｍ＞と等しくない限り、変更することができる。

・共用キーの下でデータを送信する実体のグループの各メンバにＩＤ１０６によって名前を付けるのに十分なビット数を使用しなければならない。たとえば、２つの実体が共用キーを使用して互いにメッセージを送ろうとする場合、１ビットで十分であり、２つの実体の一方が"０"という名前になり、他方が"１"という名前になる。

【００２４】パイプライン化も、上記の技法に簡単に適合させることができる。一部のＤＥＳエンジンは、複数の内部的に刻時される段を有し、暗号化アルゴリズムを実行する時に、所与の段のデータが後続の段に転送される。ワードは互いに独立に暗号化できるので、パイプライン式暗号化手法が可能である。ここで図５を参照すると、単一の多段ＤＥＳエンジンが示されている。このＤＥＳエンジンは、図５では、破線で示した４つの段を有する。たとえば、各段は、４ラウンドのＤＥＳ計算を含むことができる。時刻０に、ワード１がＤＥＳエンジンに提示され、暗号化処理を受ける。時刻１に、ワード１（Ｗ１）がこのＤＥＳエンジンの内部の第２段に移り、ワード２（Ｗ２）がこのエンジンの第１段に提示される。時刻２には、ワード１がこのＤＥＳエンジンの内部の第３段に移り、ワード２が内部の第２段に移り、ワード３（Ｗ３）がこのエンジンの第１段に提示される。同様にして時刻３には、ワード１がこのＤＥＳエンジンの内部の第４段に移り、ワード２が内部の第３段に移り、ワード３が内部の第２段に移り、ワード４（Ｗ４）がこのエンジンの第１段に提示される。最後に、時刻４に、ワード１がＤＥＳ暗号化を終えてこのエンジンから出、ワード５（Ｗ５）がこのエンジンの第１段に提示される。暗号化されるワードはそれぞれ、他のワードの暗号化された値に依存しないので、段間で別個の動作が可能な独立の内部段を有するＤＥＳエンジンを使用すると、

13

独立の暗号化動作をこのパイプライン方式で実行することができる。

【００２５】図６は、並列ＭＡＣ方式を使用して、高速のメッセージ・ジェネレータ１６と低速の擬似乱数関数に基づくサイン処理２２の間で帯域幅を一致させる方法を示すタイミング図である。図６のタイミングに関して、４つのＤＥＳエンジン１３４、１３６、１３８、１４０が送信元と受信先の両方で使用可能な、図７の実施態様を仮定する。さらに、メッセージ１３０は、１単位時間毎に３２ビット・ワード１個の割合で生成されているが、基礎となるＤＥＳエンジンは、４単位時間毎に６４ビット・ワード１つの割合でしか暗号化できないと仮定する。このタイミング図では、２つのワードの排他的論理和、ワードの連結、カウンタの増分、カウンタの更新などに必要な時間を無視しているが、それらの時間は、一般に、暗号化動作の実行に必要な時間よりはるかに短い。図７の装置は、４つのＤＥＳエンジン（１３４、１３６、１３８、１４０）を使用し、認証されるメッセージの長さとは無関係に、その待ち時間は単一のＤＥＳエンジンの待ち時間にすぎない。したがって、この並列化によって、メッセージ長が長い時に、従来の方法に比べて大きなスループットの利益が得られる。

【００２６】これから図７に示された装置に関して、図６を詳細に説明する。時刻０に、符号化されたＩＤ１０６（図７）とＣＴＲ１０４が、制御論理機構１３２によってＤＥＳエンジン１（図７の１３４）に提示される。また、時刻０に、好ましい実施例では６４ビットである一時変数Ｔ（図７の１１４）が、全ビット０に初期設定される。暗号テキスト１５０（図７）は、時刻０＋４＝４にＤＥＳエンジン１（図７の１３４）から出る（前提の１つとして、前述のようにＤＥＳ暗号化エンジンに４時間単位を要するものとする）。この時、暗号テキスト１５０は、ブロック１４６で移動タグＴ（図７の１１４）の現在値と排他的論理和をとられる。

【００２７】時刻１に、メッセージ１３０（図７）のワード１（図７の１５２）が、図７の制御論理機構１３２によって符号化され（先に図４に関して説明した符号化）、ＤＥＳエンジン２（図７の１３６）に提示され、時刻１＋４＝５にそこから出る。この時、結果として得られる暗号テキスト１５２が、ブロック１４６で、Ｔ（図７の１４４）の現在値と排他的論理和をとられる。

【００２８】時刻２に、メッセージのワード２（図７の１５４）が符号化され、ＤＥＳエンジン３（図７の１３８）に提示される。これは時刻２＋４＝６に出る。この時、結果として得られる暗号テキスト１５４が、ブロック１４６で、Ｔ（図７の１４４）の現在値と排他的論理和をとられる。

【００２９】時刻３に、メッセージのワード３（図７の１５６）が符号化され、ＤＥＳエンジン４（図７の１４０）に提示される。これは時刻３＋４＝７に出る。この

14

時、結果として得られる暗号テキスト１５６が、ブロック１４６で、Ｔ（図７の１４４）の現在値と排他的論理和をとられる。

【００３０】時刻４に、ＤＥＳエンジン１（図７の１３４）は、ＩＤとＣＴＲの符号化を処理し終えたばかりであり、ワード４（図７の１５８）が準備ができている。このワード４がＤＥＳエンジン１（図７の１３４）に提示され、時刻４＋４＝８にそこから出る。この時、その暗号テキストが、ブロック１４６で、Ｔ（図７の１４４）の現在値と排他的論理和をとられる。

【００３１】メッセージ１３０の７つのワードがすべて処理されるまで、この処理が継続する。

【００３２】この図では、メッセージの最後のワード（図７に１６０として示されるワード７）は、時刻７にＤＥＳエンジン４（図７の１４０）に入る。暗号テキスト１５６は、時刻７＋４＝１１に出る時、ブロック１４６でＴ（図７の１４４）の現在値と排他的論理和をとられる。その結果は、ブロック１４８で切り捨てられ、あるいはそのまま残されるが、メッセージ１３０全体のタグ１１４である。

【００３３】図９は、すべて共通のデータ経路またはバス１７２を介して相互接続された、ＣＰＵ１７０、読取専用メモリ（ＲＯＭ）１７６、ランダム・アクセス・メモリ（ＲＡＭ）１７４、入出力アダプタ１７８、ユーザ・インターフェース・アダプタ１８２、通信アダプタ１９４、認証アダプタ１９５および表示装置アダプタ１９６を含む、上記の動作を実行するための、好ましい実施例のデータ処理システム１６８を示す図である。上記の構成要素がそれぞれ、ＣＰＵをバス・マスタとし、特定のアドレス範囲をシステム内の各構成要素専用にするなどの方法を含む、当業者に既知の普通の技法を使用して、共通のバスにアクセスする。当業者に既知の他の普通の技法には、ＤＡＳＤ１８０やネットワーク２００などの外部装置からデータ処理システムのランダム・アクセス・メモリ（ＲＡＭ）１７４へ高速でデータを転送するのに使用される直接メモリ・アクセス（ＤＭＡ）が含まれる。図９からわかるように、外部装置であるＤＡＳＤ１８０は入出力アダプタ１７８を介し、ネットワーク２００は通信アダプタ１９４を介して、共通のバス１７２にインターフェースする。表示装置１９８など他の外部装置も、同様に表示装置アダプタ１９６を使用して、バス１７２と表示装置１９８の間のデータ・フローを実現する。ユーザ・インターフェース手段は、ユーザ・インターフェース・アダプタ１８２によって提供される。ユーザ・インターフェース・アダプタ１８２には、ジョイスティック１９２、マウス１８６、キーボード１８４、スピーカ１８８などが接続されている。これらの装置はそれぞれ周知であり、したがって本明細書では詳細には説明しない。

【００３４】図９は、下記のように図１に対応する。図

９のネットワーク２００は、機密保護されないチャネル２０に対応する。図１の送信元１２内の諸機能は、図９のデータ処理システム１６８と認証アダプタ１９５によって提供される。認証アダプタ１９５は、図７に示した論理機構および対応する回路を含む。代替実施例では、認証アダプタ１９５を通信アダプタ１９４と組み合わせて、さらに性能を高めることができる。図１の受信先１４内の諸機能は、図９のデータ処理システム１６８と同一タイプまたは異なるタイプの別のデータ・プロセッサによって提供される。

【００３５】以下のように発明を開示する。

（１）データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせて、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【００３６】（２）前記擬似乱数関数が、データ暗号化標準（ＤＥＳ）アルゴリズムであることを特徴とする、（１）の方法。

【００３７】（３）前記ブロックが、固定長であることを特徴とする、（１）の方法。

【００３８】（４）前記組み合わせステップが、排他的論理和演算を含むことを特徴とする、（１）の方法。

【００３９】（５）前記タグが、切捨てその他の方法によって所与の長さに短縮されることを特徴とする、（１）の方法。

【００４０】（６）前記擬似乱数関数が、多段式であることを特徴とする、（１）の方法。

【００４１】（７）前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、（６）の方法。

【００４２】（８）前記複数のワードが、前記複数の多段式擬似乱数関数に同時に提示されることを特徴とする、（１）の方法。

【００４３】（９）さらに、少なくとも前記タグを前記識別子と組み合わせて、メッセージ認証コード（ＭＡＣ）を作成するステップを含む、（１）の方法。

【００４４】（１０）さらに、少なくともデータとメッセージ認証コードとを組み合わせて、データ・パケットを作成するステップを含む、（９）の方法。

【００４５】（１１）データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、（ｉ）前記ワードのそれぞれと（ii）前記データのヘッダとに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせて、メッセージ認証コード（ＭＡＣ）を作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【００４６】（１２）前記擬似乱数関数が、データ暗号化標準（ＤＥＳ）アルゴリズムであることを特徴とする、（１１）の方法。

【００４７】（１３）前記ブロックが、固定長であることを特徴とする、（１１）の方法。

【００４８】（１４）前記組み合わせステップが、排他的論理和演算を含むことを特徴とする、（１１）の方法。

【００４９】（１５）前記ヘッダが、識別子とカウンタとを含むことを特徴とする、（１１）の方法。

【００５０】（１６）前記タグが、切捨てによって所与の長さに短縮されることを特徴とする、（１１）の方法。

【００５１】（１７）前記擬似乱数関数が、多段式であることを特徴とする、（１１）の方法。

【００５２】（１８）前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、（１７）の方法。

【００５３】（１９）前記複数のワードが、前記複数の多段式擬似乱数関数に同時に提示されることを特徴とする、（１１）の方法。

【００５４】（２０）さらに、少なくとも前記タグを前記識別子と組み合わせて、メッセージ認証コード（ＭＡＣ）を作成するステップを含む、（１１）の方法。

【００５５】（２１）さらに、少なくともデータとメッセージ認証コードとを組み合わせて、データ・パケットを作成するステップを含む、（２０）の方法。

【００５６】（２２）データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせて、タグを作成するステップと、少なくとも前記データと前記タグとを組み合わせて、データ・パケットを作成するステップと、非機密保護通信チャネルを介して前記データ・パケットを送信するステップと、データ・パケットを受信するステップと、データ・パケットを分解して、タグとデータを抽出するステップと、少なくとも抽出されたデータと局所キーとから第２タグを生成するステップと、抽出されたタグと第２タグを比較して、データ・パケットのデータ信頼性を判定するステップとを含む、非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【００５７】（２３）データを複数のブロックに区分するステップと、前記ブロックのそれぞれにブロック識別

子を連結して、ワードを作成するステップと、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせて、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【００５８】（２４）前記ブロック識別子が、ブロック・インデックスに基づくことを特徴とする、（２３）の方法。

【００５９】（２５）前記擬似乱数関数が、多段式であることを特徴とする、（２３）の方法。

【００６０】（２６）前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、（２５）の方法。

【００６１】（２７）データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、（ｉ）前記ワードのそれぞれと（ii）前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせて、タグを作成するステップと、少なくともデータとタグとを組み合わせて、データ・パケットを作成するステップと、非機密保護通信チャネルを介してデータ・パケットを送信するステップと、データ・パケットを受信するステップと、受信したデータ・パケットを分解して、受信データと受信タグを抽出するステップと、少なくとも受信データと局所キーとから局所タグを生成するステップと、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【００６２】（２８）データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、（ｉ）前記ワードのそれぞれと（ii）前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせて、タグを作成するステップと、少なくともデータ、タグ、送信元識別子および時間変動パラメータを組み合わせて、データ・パケットを作成するステップと、非機密保護通信チャネルを介してデータ・パケットを送信するステップと、データ・パケットを受信するステップと、受信データ・パケットを分解して、受信データ、受信タグ、受信送信元識別子および受信時間変動パラメータを抽出するステップと、少なくとも受信データ、受信送信元識別子、受信時間変動パラメータおよび局所キーから局所タグを生成するステップと、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性

を判定するステップとを含む、前記非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【００６３】（２９）前記比較ステップが、さらに、前記受信時間変動パラメータを局所時間変動パラメータと比較して、前記データ信頼性をさらに判定するステップを含むことを特徴とする、（２８）の方法。

【００６４】（３０）前記受信時間変動パラメータが、受信カウンタを含むことを特徴とする、（２９）の方法。

【００６５】（３１）前記受信時間変動パラメータが、タイム・スタンプを含むことを特徴とする、（２９）の方法。

【００６６】（３２）前記受信時間変動パラメータが、シーケンス番号を含むことを特徴とする、（２９）の方法。

【００６７】（３３）データを複数のブロックに区分するステップと、前記ブロックのそれぞれにブロック識別子を連結して、ワードを作成するステップと、（ｉ）前記ワードのそれぞれと（ii）前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせて、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【００６８】（３４）受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出するステップと、少なくとも受信データ、受信時間変動パラメータおよび局所キーから局所タグを生成するステップと、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、受信データ・パケットの信頼性を判定するための方法。

【００６９】（３５）前記受信時間変動パラメータが、受信カウンタを含むことを特徴とする、（３４）の方法。

【００７０】（３６）前記受信時間変動パラメータが、タイム・スタンプを含むことを特徴とする、（３４）の方法。

【００７１】（３７）前記受信時間変動パラメータが、シーケンス番号を含むことを特徴とする、（３４）の方法。

【００７２】（３８）前記受信データ・パケットが、さらに送信元識別子を含むことを特徴とする、（３４）の方法。

【００７３】（３９）さらに、前記送信元識別子を使用して、局所テーブルから前記局所キーを取得するステップを含む、（３８）の方法。

【００７４】（４０）データを複数のブロックに区分する手段と、前記ブロックのそれぞれを符号化して、前記ブロックのそれぞれの値と前記ブロックのそれぞれの識

19

別子との両方を表すワードを作成する手段と、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、前記複数の暗号ワードを組み合わせて、タグを作成する手段とを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するためのシステム。

【００７５】（４１）データを複数のブロックに区分する手段と、前記ブロックのそれぞれにブロック識別子を組み合わせて、ワードを作成する手段と、（ｉ）前記ワードのそれぞれと（ii）前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、前記複数の暗号ワードを組み合わせて、タグを作成する手段とを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するためのシステム。

【００７６】（４２）受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出する手段と、少なくとも受信データ、受信時間変動パラメータおよび局所キーから局所タグを生成する手段と、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定する手段とを含む、受信データ・パケットの信頼性を判定するためのシステム。

【００７７】（４３）前記受信データ・パケットが、さらに送信元識別子を含むことを特徴とする、（４２）のシステム。

【００７８】（４４）さらに、前記送信元識別子を使用して、局所テーブルから前記局所キーにアクセスする手段を含む、（４３）のシステム。

【００７９】（４５）データを複数のブロックに区分する手段と、前記ブロックのそれぞれを符号化して、前記ブロックのそれぞれの値と前記ブロックのそれぞれの識別子との両方を表すワードを作成する手段と、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、前記複数の暗号ワードを組み合わせて、タグを作成する手段とを含む、コンピュータ互換媒体上に常駐する、通信チャネルを使用したデータの転送と共に使用する認証タグをデータ処理システムが決定できるようにするためのコンピュータ・プログラム。

【００８０】（４６）データを複数のブロックに区分する手段と、前記ブロックのそれぞれにブロック識別子を組み合わせて、ワードを作成する手段と、（ｉ）前記ワードのそれぞれと（ii）前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、前記複数の暗号ワードを組み合わせて、タグを作成する手段とを含む、コンピュータ互換媒体上に常駐する、通信チャネルを使用したデータの転送と共に使用する認証タグをデータ処理システムが決定できるようにするためのコンピュータ・プログラム。

【００８１】（４７）受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出する手段と、少なくとも受信データ、受信時間

20

変動パラメータおよび局所キーから局所タグを生成する手段と、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定する手段とを含む、コンピュータ互換媒体上に常駐する、受信データ・パケットの信頼性をデータ処理システムが判定できるようにするためのコンピュータ・プログラム。

【００８２】

【発明の効果】本発明により、簡単、高速かつ安全にメッセージ認証コード（ＭＡＣ）を計算する方法が提供される。

【図面の簡単な説明】

【図１】送信されたメッセージの保全性を保護するデータ通信システムのシステム全体図である。

【図２】通信媒体を使用して転送されるメッセージにサインするための処理を示す図である。

【図３】受信したメッセージを認証するための処理を示す図である。

【図４】データ処理システム内の送信元または受信先のタグ計算の機能を示す図である。

【図５】パイプライン式に使用される多段式ＤＥＳエンジンを示す図である。

【図６】データ認証で使用されるタグの計算に関するタイミング図である。

【図７】データ処理システム内の送信元または受信先のＭＡＣ計算を物理的に示す図である。

【図８】サイン付きメッセージの構造を示す図である。

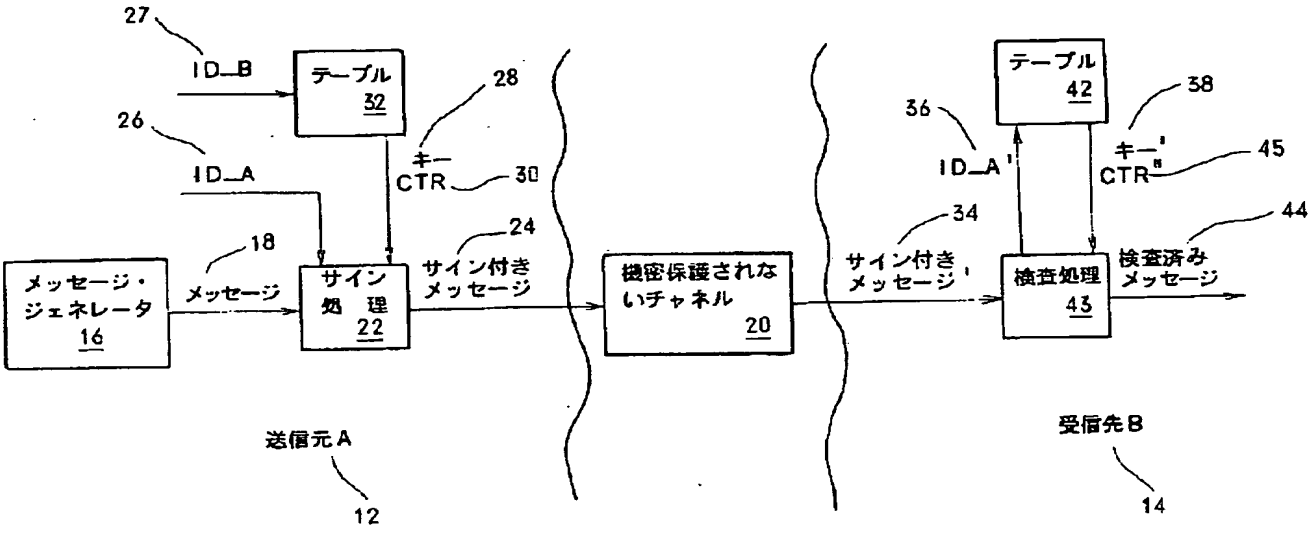
【図９】代表的なデータ処理システムを示す図である。

【図１０】逐次式のメッセージ認証コード判定技法を示す図である。

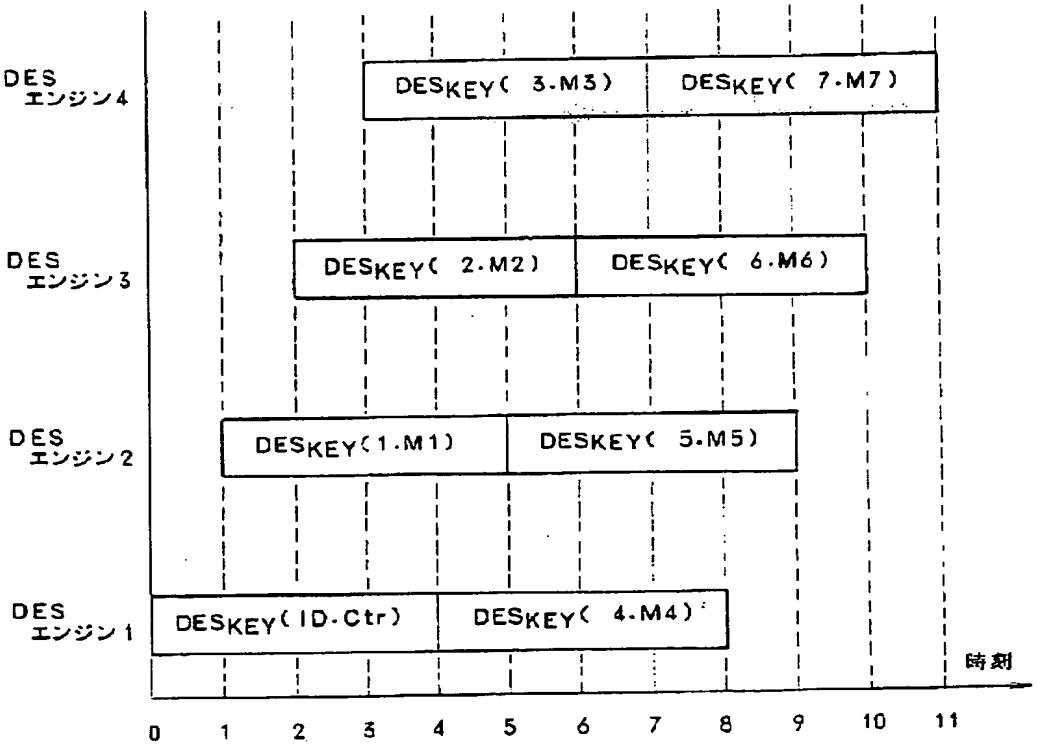
【符号の説明】

１２　送信元
１４　受信先
１６　メッセージ・ジェネレータ
１８　メッセージ
２０　機密保護されないチャネル
２２　サイン処理
２４　サイン付きメッセージ
２６　送信元識別子（ＩＤ＿Ａ）
２７　受信先識別子（ＩＤ＿Ｂ）
２８　キー（ｋｅｙ）
３０　カウンタ（ＣＴＲ）
３２　テーブル
３４　サイン付きメッセージ'
３６　署名者識別子（ＩＤ＿Ａ'）
３８　キー'（ｋｅｙ'）
４０　カウンタ'（ＣＴＲ'）
４２　テーブル
４３　検査処理
４４　検査済みメッセージ

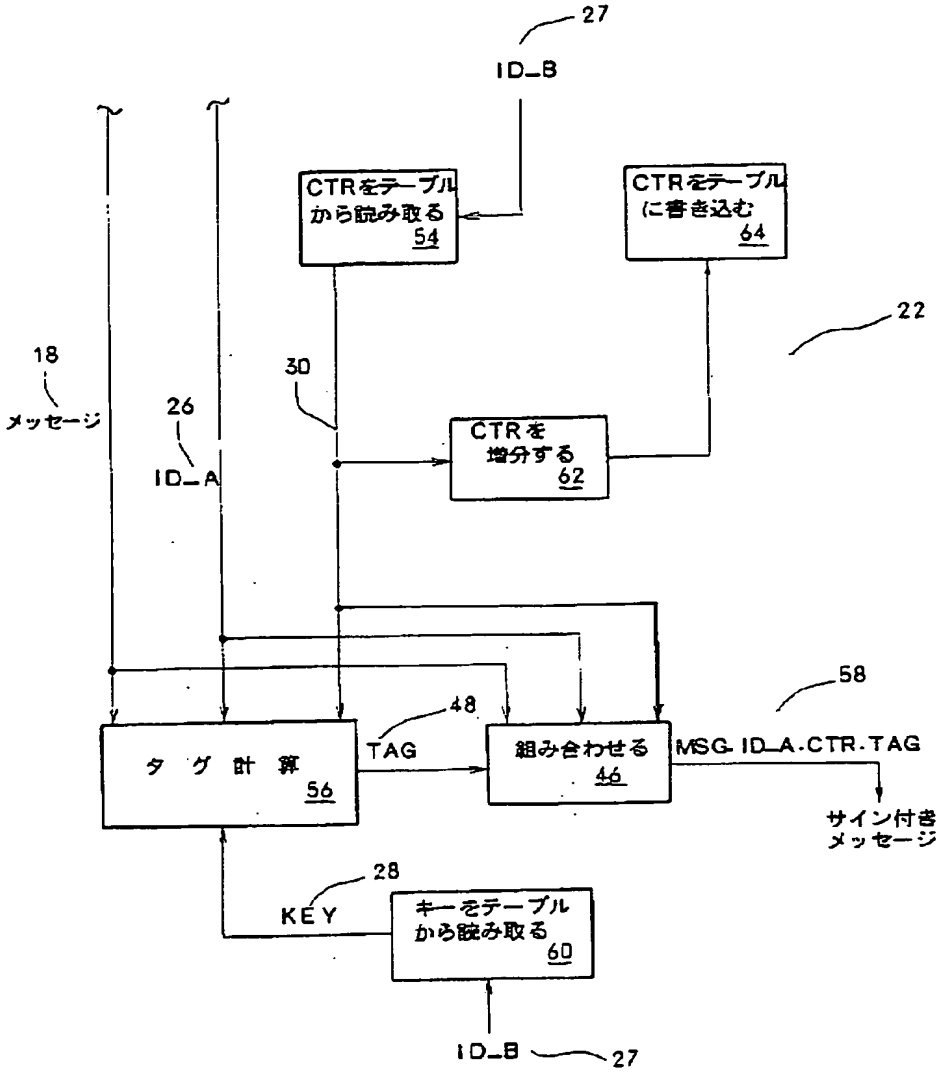
【図１】


27
ID_B
テーブル
32
28
キー
CTR
30
26
ID_A
18
メッセージ・
ジェネレータ
16
メッセージ
サイン
処理
22
24
サイン付き
メッセージ
機密保護されない
チャネル
20
テーブル
42
38
36
ID_A'
キー'
CTR''
45
34
サイン付き
メッセージ'
検査処理
43
44
検査済み
メッセージ
送信元A
12
受信先B
14

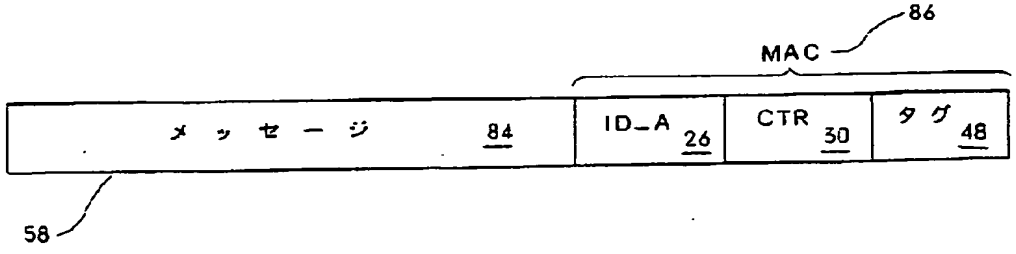
【図６】


DES
エンジン4
DESKEY(3.M3)
DESKEY(7.M7)
DES
エンジン3
DESKEY(2.M2)
DESKEY(6.M6)
DES
エンジン2
DESKEY(1.M1)
DESKEY(5.M5)
DES
エンジン1
DESKEY(ID.Ctr)
DESKEY(4.M4)
時刻
0
1
2
3
4
5
6
7
8
9
10
11

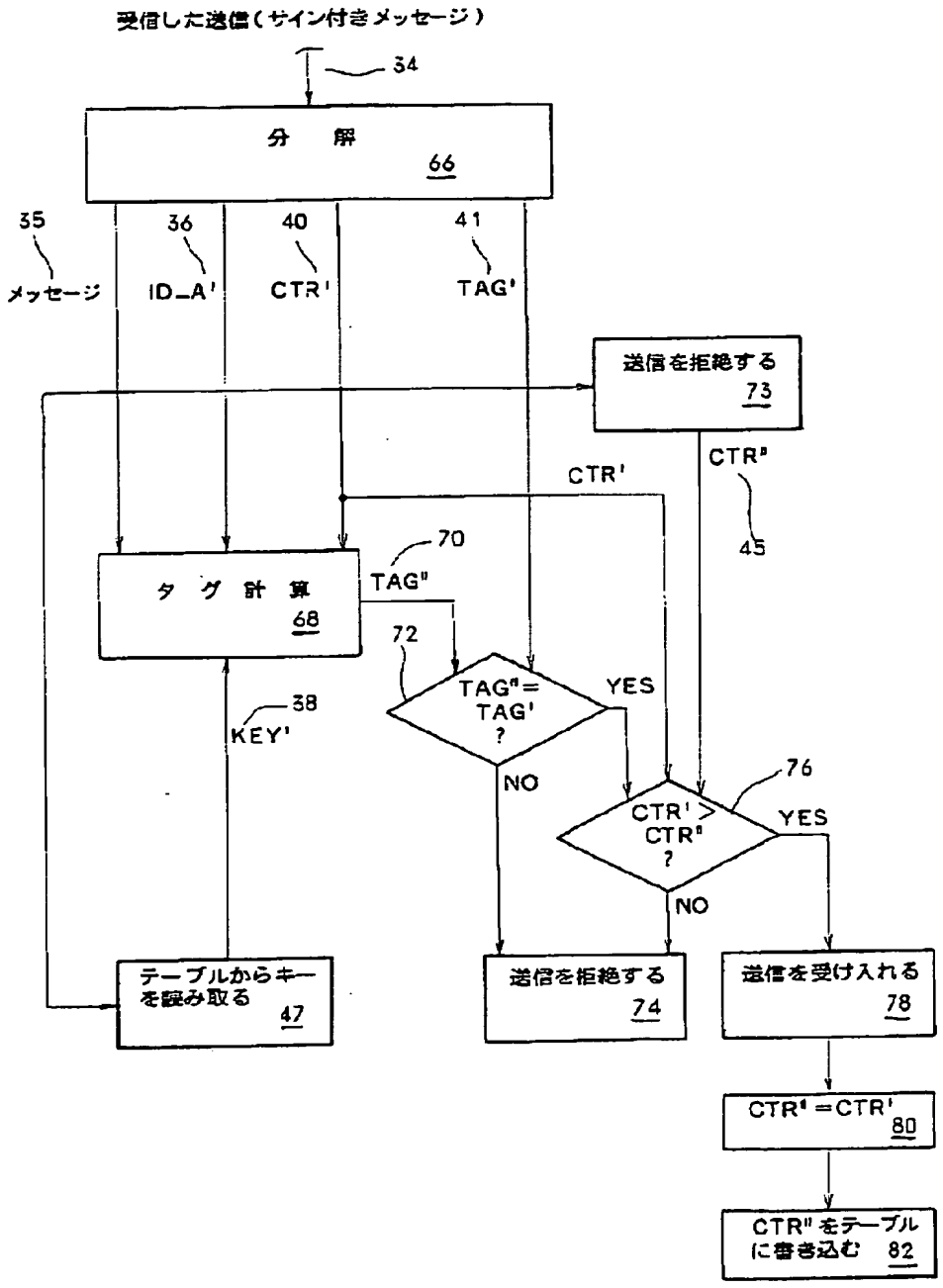
【図2】


27
ID_B
CTRをテーブルから読み取る 54
CTRをテーブルに書き込む 64
22
18
メッセージ
30
26
ID_A
CTRを増分する 62
58
48
タグ計算 56
TAG
組み合わせる 46
MSG.ID_A.CTR.TAG
サイン付きメッセージ
28
KEY
キーをテーブルから読み取る 60
ID_B
27

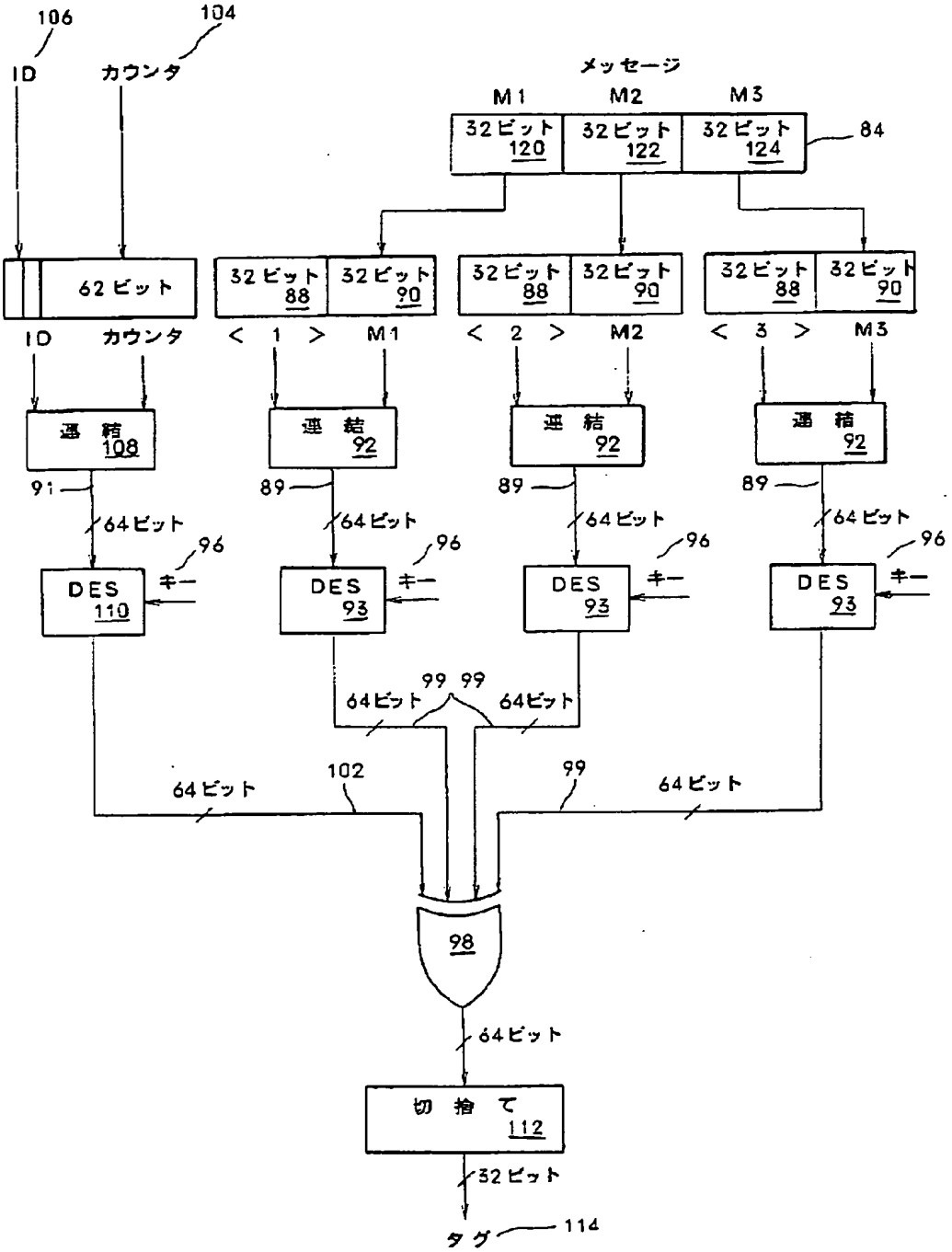
【図8】


86
MAC
メッセージ 84
ID_A 26
CTR 30
タグ 48
58

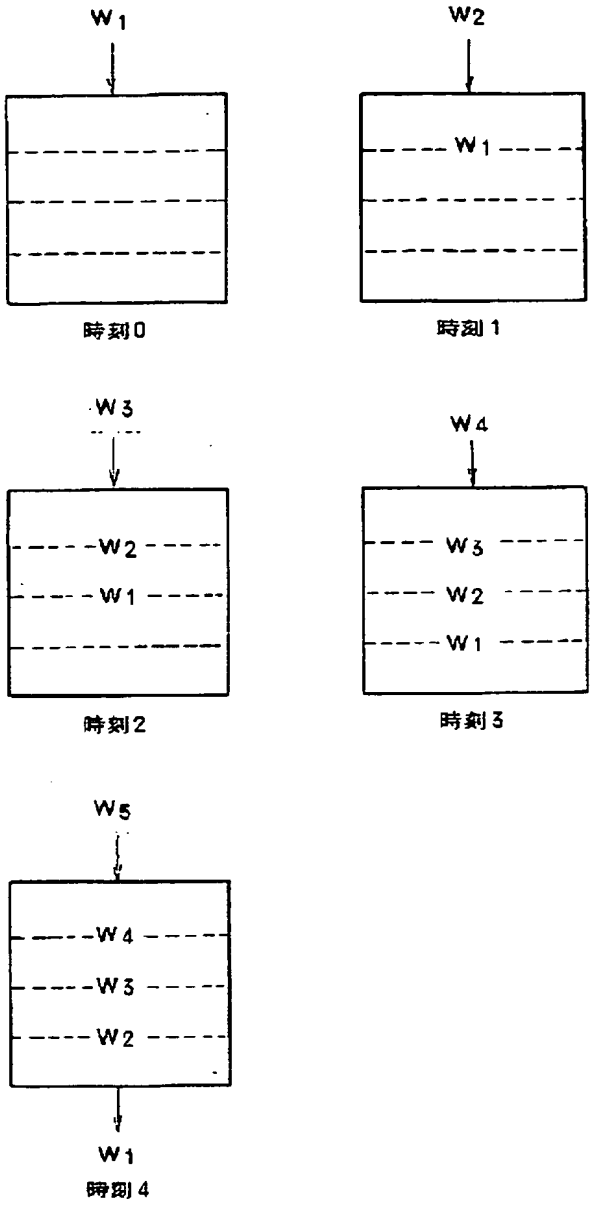
【図３】


受信した送信（サイン付きメッセージ）
34
分　解
66
35
メッセージ
36
ID_A'
40
CTR'
41
TAG'
送信を拒絶する
73
CTR'
CTR"
45
70
タ グ 計 算
68
TAG"
72
TAG"=
TAG'
?
YES
NO
38
KEY'
76
CTR'>
CTR"
?
YES
NO
テーブルからキー
を読み取る
47
送信を拒絶する
74
送信を受け入れる
78
CTR"=CTR'
80
CTR"をテーブル
に書き込む
82

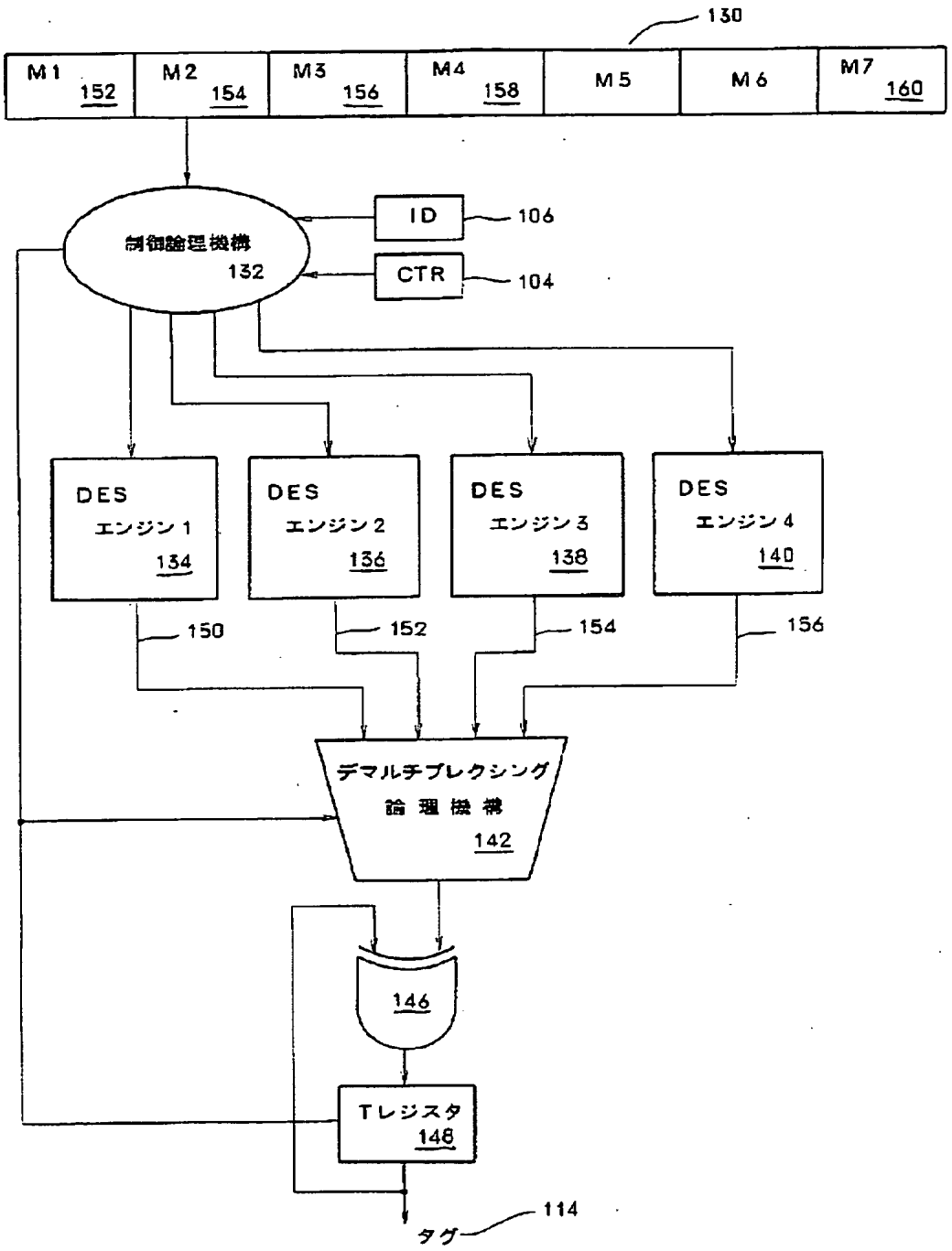
【図４】


106
104
ID
カウンタ
メッセージ
M1
M2
M3
32ビット 120
32ビット 122
32ビット 124
84
62ビット
32ビット 88
32ビット 90
ID
カウンタ
< 1 > M1
< 2 > M2
< 3 > M3
連結 108
連結 92
91
89
64ビット
96
DES 110
DES 93
キー
99
102
98
切捨て 112
32ビット
タグ
114

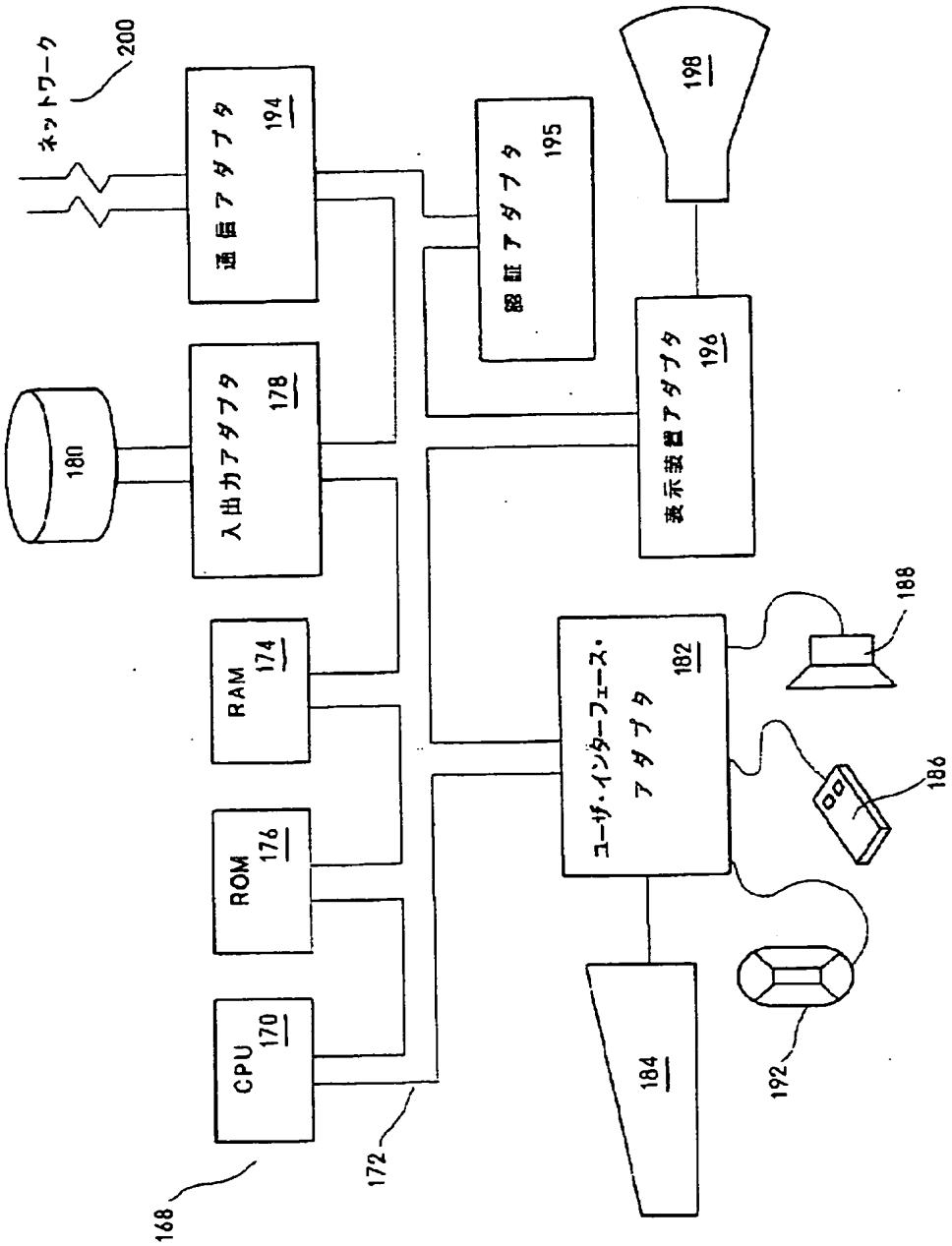
【図5】



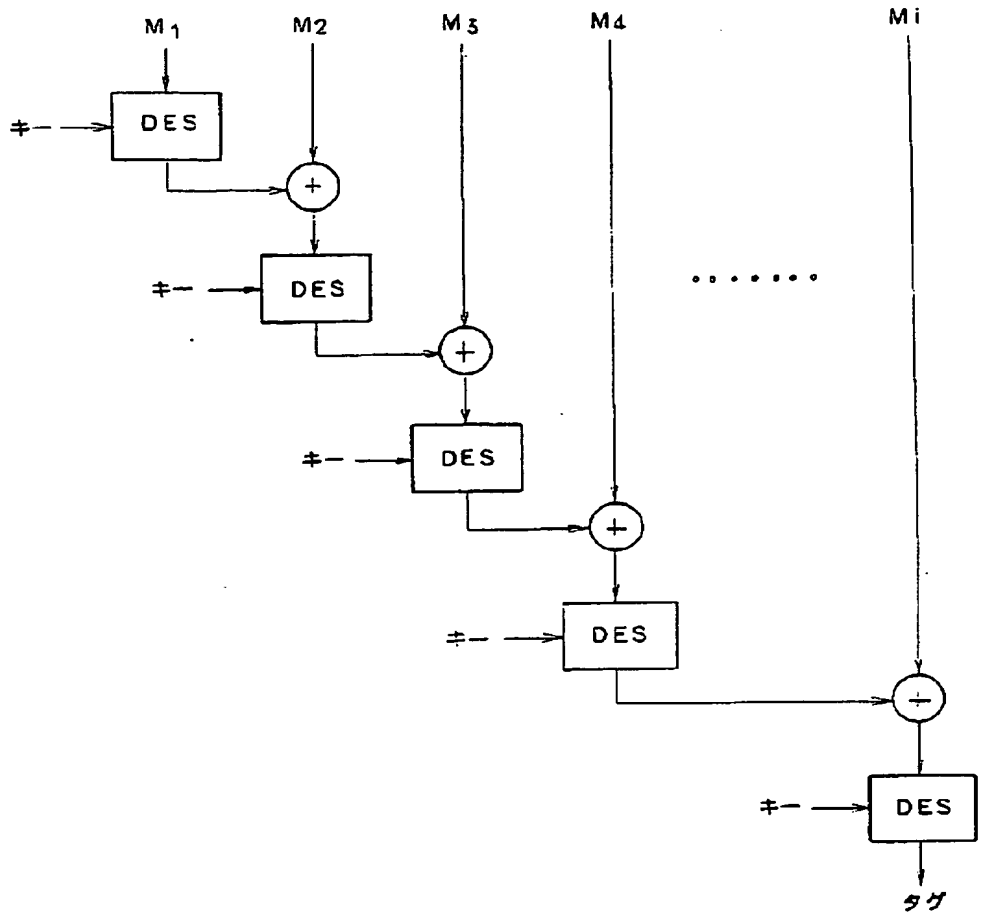
【図7】


130
M1 152
M2 154
M3 156
M4 158
M5
M6
M7 160
制御論理機構 132
ID
106
CTR
104
DES エンジン1 134
DES エンジン2 136
DES エンジン3 138
DES エンジン4 140
150
152
154
156
デマルチプレクシング論理機構 142
146
Tレジスタ 148
タグ
114

【図9】


ネットワーク
200
通信アダプタ
194
認証アダプタ
195
198
入出力アダプタ
178
180
表示装置アダプタ
196
RAM
174
ユーザ・インターフェース・
アダプタ
182
188
186
ROM
176
CPU
170
184
192
172
168

【図10】



フロントページの続き

(72)発明者　ロッシュ・アンドレ・ゲラン
アメリカ合衆国10598　ニューヨーク州ヨークタウン・ハイツ　ロシャンボー・ドライブ　シーニック・ビュー　ナンバー4エイチ

(72)発明者　フィリップ・ウォルダー・ロガウェイ
アメリカ合衆国78758　テキサス州オースチン　クリプル・クリーク・ドライブ1620

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.